

FILED
LODGEDENTERED
RECEIVED

AO 106 (Rev. 04/10) Application for Search Warrant (Modified: WAWD 10-26-18)

NOV 06 2019

UNITED STATES DISTRICT COURT

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTYfor the
Western District of Washington

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 Cellular Telephone Numbers assigned to T-Mobile
 Wireless and Onvoy LLC, as further described in
 Attachments A-1 and A-2

Case No.

MJ19-541

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, attached hereto and incorporated by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


Code Section	Offense Description
18 U.S.C. § 371	Conspiracy to Engage in Cyberstalking.
18 U.S.C. § 2 & 2261A(2)(A)	Interstate Stalking.

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Greg Leiman, attached hereto and incorporated herein by reference.

- ☒ Delayed notice of 60 days (give exact ending date if more than 30 days: Jan. 5, 2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.




Applicant's signature

Greg Leiman, Special Agent FBI

Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: Nov. 6, 2019


Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge

Printed name and title

ATTACHMENT A-1

**Target Cell Phone-
Records**

This warrant applies to information associated with the cellular telephone assigned call numbers **206-430-4163** and **206-549-9854** (hereinafter “**Target Cell Phones**”), that is stored at the premises owned, maintained, controlled, and/or operated by T-Mobile Wireless, a wireless telephone service provider headquartered at 3625 132nd Avenue S.E., Bellevue, Washington 98006.

ATTACHMENT A-2

**Target Cell Phone-
Records**

This warrant applies to information associated with the cellular telephone assigned call numbers **206-457-0982** (hereinafter “**Target Cell Phone**”), that is stored at the premises owned, maintained, controlled, and/or operated by Onvoy LLC, a wireless telephone service provider headquartered at 10300 6th Avenue North, Plymouth, Minnesota 55441.

ATTACHMENT B

Particular Things to be Seized

A. The following information about the customers or subscribers of the Accounts of the Target Cell Phones as further described in Attachments A-1 and A-2:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account numbers) and billing records.

B. All records and other information (not including the contents of communications) relating to the Account, including:

9. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet

Protocol Addresses; cookie IDs; browser type;

10. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers), and;

11. All information about the location of each of the Target Cell Phones described in Attachment A from October 20, 2018, through October 27, 2018, during all times of day and night, and the status of the device and the account associated with the device (i.e., whether the device is active or operational and whether the account is in good standing, canceled, suspended, etc.). "Information about the location of the Target Cell Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

12. Specifically and including but not limited to:

- a. All call detail records with cell sites to include those cell towers and sectors utilized for voice, SMS, and data connections to include VoLTE connections;
- b. All SMS detail and content;
- c. All internet activity/DATA connections (1xRTT, EVDO, and LTE);
- d. IP sessions and destinations;
- e. Subscriber, device, account notes, billing information, and additional numbers assigned to the Account and/or devices;
- f. All device identifying information (IMEI/MEID/ESN/WIFI MAC Address, Make and Model, Point of Purchase, Point of Sale);
- g. All international roaming reports to include Country Code, Network Code, and cell towers being used;

- h. All RTT data for 1xRTT, EVDO and LTE;
- i. All Per Call Measurement Data (voice, SMS, and data/1XRTT, EVDO and LTE) (Sprint);
- j. All Network Extender reports
- k. Any and all historical GPS location information often referred to as NELOS (ATT) and/or any information to show the historical estimated location of the Target Cell Phone; and,
- l. Any and all True Call reports and data sessions (T-Mobile).

13. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of (wireless provider) (hereinafter "Provider"), Provider is required to disclose the Location Information to the government. In addition, Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Provider's services. The government shall compensate Provider for reasonable expenses incurred in furnishing such facilities or assistance.

14. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds it reasonable necessity for the seizure of the Location Information. See 18 U.S.C § 3103a(b)(2).

AFFIDAVIT

STATE OF WASHINGTON)
) ss
 COUNTY OF KING)

I, Gregory Leiman, having been duly sworn, state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since 2014. During my time as a Special Agent, I have participated in investigations pertaining to hate crimes, arson, and other federal criminal violations. I have also completed the New Agents Training Course at the FBI Academy in Quantico, Virginia. Based on my training and experience, I am familiar with the utilization and analysis of telephone toll records, geo-location data, utility records, financial records, and review of cellular telephone, computer, and digital device records and materials. I also conduct training courses to cadets at the Washington State Criminal Justice Training Center on federal civil rights, including hate crimes and color of law violations.

II. PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), to require information associated with the following telephone numbers that are stored at premises controlled by an electronic communications service and remote computer service provider, namely:

- a. **T-Mobile Wireless**, a wireless telephone service provider headquartered at 3625 132nd Ave SE, Bellevue, Washington 98006, for information about the historical location from October 20, 2018 through October 27, 2018, of the cellular telephone assigned call number 206-430-4163 and 206-549-9854.
- b. **Onvoy LLC**, a wireless telephone service provider headquartered at 10300 6th Avenue North, Plymouth, Minnesota 55441, for information about the

1 historical location from October 20, 2018 through October 27, 2018, of the
2 cellular telephone assigned call number 206-457-0982.

3 Collectively, I will refer to these phone numbers in this affidavit as the "**Target Cell**
4 **Phones.**"

5 3. More specifically, I am requesting warrants for the **Target Cell Phones** to
6 receive historical data and other records in order to ascertain the user or users'
7 movements between October 20, 2018, through October 27, 2018, when using any one or
8 more of the **Target Cell Phones**. This will assist the investigation in locating and
9 securing evidence and instrumentalities related to criminal activity described and
10 referenced herein and a criminal investigation occurring in this judicial district, and
11 potentially identify other criminal suspects or coconspirators. Further, the users' location
12 is relevant to his/her participation in some of the acts committed to facilitate the crimes
13 charged and under investigation.

14 4. Based on my training and experience and the facts as set forth in this
15 affidavit, there is probable cause to believe that violations of Title 18, United States
16 Code, Sections: 249 (hate crimes), 2261A (stalking), and 371 (conspiracy), were
17 committed by persons in possession of the **Target Cell Phones** believed to have been
18 used by CHRISTIAN FREDY DJOKO (hereafter "DJOKO") and others known and
19 unknown to the investigation. There is also probable cause to search the information
20 described in Attachments A-1 and A-2 for the items described in Attachment B to assist
21 in obtaining possession of evidence, instrumentalities, contraband or fruits of these
22 crimes.

23 5. The facts set forth in this Affidavit are based on my own personal
24 knowledge; knowledge obtained from other individuals during my participation in this
25 investigation, including other law enforcement personnel and computer scientists; review
26 of documents and records related to this investigation; communications with others who
27 have personal knowledge of the events and circumstances described herein; and
28 information gained through my training and experience. Because this Affidavit is

1 submitted for the limited purpose of establishing probable cause in support of the
 2 application for a warrant, it does not set forth each and every fact that I or others have
 3 learned during the course of this investigation.

4 **III. JURISDICTION**

5 6. This Court has jurisdiction to issue the requested warrant because it is “a
 6 court of competent jurisdiction,” as defined by 18 U.S.C. §§ 2703(a),
 7 2703(b)(1)(A), 2703(c)(1)(A), and 2711. Specifically, the Court is “a district court of the
 8 United States that – has jurisdiction over the offense[s] being investigated.” 18 U.S.C.
 9 § 2711(3)(A)(i).

10 **IV. STATEMENT OF PROBABLE CAUSE**

11 *Procedural History*

12 7. On August 1, 2019, the Grand Jury returned a two-count Indictment
 13 charging MARIE CHRISTINE FANYO-PATCHOU, RODRIGUE FODJO KAMDEM,
 14 and DJOKO with Conspiracy to Engage in Cyberstalking in violation of Title 18, United
 15 States Code, Section 371 (Count 1), and Interstate Stalking in violation of Title 18,
 16 United States Code, Sections 2 and 2261A(2)(A) and (2)(B) (Count 2). *See United States*
 17 *v. Fanyo-Patchou, et al.*, CR19-146JCC, Docket Number 1. As alleged in the Indictment,
 18 between September and November 2, 2018, the Defendants used a variety of electronic
 19 communications applications, including Facebook and WhatsApp, to harass and
 20 intimidate John Doe. In addition to threatening communications made directly to John
 21 Doe, the Defendants conspired to distribute and disseminate intimate materials about
 22 John Doe’s sexual orientation to other members of the Cameroonian community and John
 23 Doe’s family member.

24 8. The trial date is currently scheduled for February 3, 2020. Defendants
 25 KAMDEM and DJOKO have been released on an appearance bond. Defendant FANYO-
 26 PATCHOU is detained pending trial.

Relevant Facts from Background of Investigation

9. The defendants and John Doe, are all from Cameroon, a country located in West Africa. According to the U.S. Department of State's Cameroon 2018 Human Rights Report, in Cameroon, consensual same-sex sexual activity is illegal and punishable by imprisonment for a term lasting between six months up to five years (*U.S. Dep't of State, Bureau of Democracy, H.R. and Lab., Cameroon 2018 Human Rights Report 35 (2018), available at <https://www.state.gov/wp-content/uploads/2019/03/Cameroon-2018.pdf>*). The report further describes that members of the Lesbian, Gay, Bisexual, Transgender, and Queer ("LGBTQ") community in Cameroon are routinely targeted for violence and threats of violence because of their real or perceived sexual orientation or gender identity. *Id.* Moreover, Amnesty International lists Cameroon as one of seven nations where discrimination against LGBTQ individuals is particularly dangerous (*7 Discriminatory (or Deadly Countries) for LGBT People*, AMNESTY INT'L, <https://www.amnestyusa.org/7-discriminatory-or-deadly-countries-for-lgbt-people/> (last visited July 21, 2019)). Thus, the Defendants' dissemination of information pertaining to John Doe's sexual orientation placed John Doe and his family members in fear of serious bodily injury. John Doe has been interviewed on several occasions by law enforcement. The following is a summary of information that John Doe provided during those interviews that is relevant to establishing probable cause for the requested warrants.

10. In approximately 2014, John Doe came to the United States on a student visa to attend school. Sometime after he arrived in the Seattle area, John Doe became involved in a relationship with another man and in approximately 2016, the two were married.

11. In or around December 2017, FANYO-PATCHOU, a friend of John Doe from Cameroon, came to visit John Doe and stayed in his apartment. The two were friends in high school and John Doe had disclosed his sexual orientation to FANYO-

1 PATCHOU at that time. Moreover, before FANYO-PATCHOU came to visit, John Doe
2 had told her that he married a man.

3 12. While FANYO-PATCHOU stayed with John Doe, she routinely remarked
4 that being gay was not right and tried to convince him to be heterosexual. At one point
5 FANYO-PATCHOU asked him what he thought would happen if members of the
6 Cameroon community learned he was gay and had a husband.

7 13. In late September 2018, John Doe told FANYO-PATCHOU that she could
8 no longer live in his residence. FANYO-PATCHOU thereafter went to stay with another
9 associate of hers, KAMDEM. Unbeknownst to John Doe, FANYO-PATCHOU took
10 with her a cell phone that John Doe had given her to use. On the phone were intimate
11 photographs of John Doe and his husband. Further, while living with John Doe, she had
12 secretly taken photos of John Doe's personal photograph collection that documented his
13 marriage. Some of these photographs were private and contained nudity.

14 14. While staying with KAMDEN, FANYO-PATCHOU showed the
15 photographs of John Doe and his husband to KAMDEM and DJOKO. At KAMDEM's
16 request, FANYO-PATCHOU sent the photographs of John Doe to KAMDEM who in
17 turn forwarded copies to DJOKO. Shortly thereafter, KAMDEM and DJOKO began
18 releasing the photographs of John Doe and his husband online to members of the
19 Cameroon community via WhatsApp and Facebook.¹ After they did so, John Doe then
20
21
22

23 ¹ Facebook is a free-access social media networking website, accessed at
24 <http://www.facebook.com>, and allows its users to establish accounts through which users
25 can share written news, photographs, videos, and other information with other Facebook
26 users, and sometimes with the general public. Similarly, WhatsApp is a social media
27 messaging application and is owned by Facebook. Both Facebook and WhatsApp allow
28 various privacy settings and allow members to create group chats to share information.
WhatsApp, however, is an encrypted application and its content can only be viewed on
the source device, i.e. cell phone or tablet. WhatsApp content and data is not retained by
Facebook or other third-party provider.

1 began receiving threatening and harassing text messages from unknown persons who
2 were using phone numbers with Cameroonian country codes.

3 15. In the course of law enforcement interviews with John Doe, he provided
4 screenshots of communications received over WhatsApp from known and unknown
5 individuals. For example, in or around late October 2018, KAMDEM used WhatsApp to
6 send John Doe a screenshot of a Facebook post made by FANYO-PATCHOU. The
7 Facebook post was in French and stated, "The faggot of Seattle needs to kill himself after
8 writing his will." John Doe also reported that he has observed postings KAMDEM and
9 DJOKO have made to Facebook, to which they attached sexual photographs of John Doe
10 and announced that John Doe is gay and "prostituting" himself. Multiple relatives further
11 reported to John Doe that they have received similar materials from KAMDEM.

12 16. On or about October 22, 2018, John Doe reported to Seattle Police
13 Department (SPD) that he had been assaulted in the early morning hours of October 21,
14 2018. John Doe advised that he was near his residence when approached by two
15 Cameroonian men, and that the men grabbed him from behind, pulled his ears, pushed
16 him down onto his knees, and called him a "faggot" and made other derogatory
17 comments about his sexual orientation. John Doe also reported that the men said, "she
18 tried to make you change but you didn't want to." John Doe interpreted this to mean that
19 he had rejected FANYO-PATCHO's attempts to convert him to be heterosexual.

20 17. On or about November 2, 2018, John Doe reported that unknown persons
21 spray-painted his vehicle with the words "Dirty" and "Fag" and images in the shape of
22 penises.

23 18. Based on SPD's preliminary investigation, KAMDEM was arrested on
24 November 3, 2018, and DJOKO was arrested on November 10, 2018, for investigation of
25 the State crime of malicious harassment. KAMDEM and DJOKO's phones were seized
26 upon their arrest, and SPD obtained search warrants to examine these devices, which
27 were authorized by a King County Superior Court Judge.
28

1 19. The initial examination of DJOKO's phone by SPD determined that no
 2 location data was contained in the device between the dates of October 11, 2018, and
 3 November 4, 2018. There was also no call or SMS text data prior to November 4, 2018.
 4 Yet, application data existed on the phone that predated November 4, 2018, meaning that
 5 the device had been used prior to November 4, 2018, to access certain digital
 6 applications. Moreover, as discussed below, an examination of KAMDEM's phone
 7 revealed WhatsApp messages between KAMDEM and DJOKO. These same messages,
 8 though, were not found on DJOKO's phone. For these reasons, and based on my training
 9 and experience, I believe that DJOKO likely deleted the location and communication data
 10 on or around November 3, 2018, when KAMDEM was arrested. DJOKO was arrested
 11 approximately one week later, on November 10, 2018.

12 20. Pursuant to the King County search warrants, law enforcement also
 13 conducted a search of KAMDEM's mobile phone and discovered communications over
 14 WhatsApp from KAMDEM to DJOKO, FANYO-PATCHOU, and other known and
 15 unknown conspirators relating to the course of conduct against John Doe. Some of these
 16 messages² include the following:

17 A. On or about September 28, 2018, DJOKO sent KAMDEM a copy of the
 18 biographic page from John Doe's passport.

19 B. On or about September 30, 2018, DJOKO and KAMDEM discussed a
 20 plan to submit a letter to immigration regarding John Doe, and DJOKO
 21 stated, "I'll send the letter to the USCIS³ as well[.] I want him to be
 22 returned to the old country for good[.]" Then, on or about October 1,
 23 2018, KAMDEM stated, "I'll reveal him[.] In the old country, the
 24 faggots are burnt at the stakes[.] He is lucky to be here[.]"

25
 26
 27 ² Messages retrieved from KAMDEM's device were primarily in West African French.
 28 Unofficial translations, by FBI personnel, of the writings in French are provided in this Affidavit.

³ USCIS refers to United States Citizenship and Immigration Service.
 AFFIDAVIT of SA Leiman- 7

1 C. On or about October 4, 2018, KAMDEM asked FANYO-PATCHOU to
2 send him all the materials she had pertaining to John Doe. Then,
3 between on or about October 16, 2018, to October 18, 2018, FANYO-
4 PATCHOU responded by sending photographs and materials about
5 John Doe and his husband, including a photograph of John Doe kissing
6 his husband, a photograph of John Doe and his husband in a hotel room,
7 and a photograph of John Doe and his husband wearing matching
8 pajamas, as well as nine additional photos.

9 D. On or about October 17, 2018, KAMDEM used WhatsApp to forward
10 several intimate images provided by FANYO-PATCHOU, along with
11 the biographic page of John Doe's passport provided by DJOKO, to an
12 individual with the moniker "Chao."

13 E. On or about November 1, 2018, DJOKO sent KAMDEM a photograph
14 of an array of printed copies of photographs of FANYO-PATCHOU
15 with John Doe, along with a printed copy of John Doe's marriage
16 certificate. DJOKO and KAMDEN discussed when to publish this
17 material, and KAMDEM said, "I posted."

18 F. On or about November 1, 2018, KAMDEM sent DJOKO a message
19 stating, "I will send you you can publish," along with a digital copy of a
20 photograph of John Doe and his husband in a hotel room. DJOKO
21 responded, "[I]t's already done on face," a likely reference to having
22 posted the photograph on Facebook.

23 21. Further investigation revealed that the **Target Cell Phones**, (206) 430-
24 4163, (206) 549-9854, (206) 457-0982 are associated and/or used by DJOKO. Pursuant
25 to the examination of KAMDEM's seized cell phone under the State search warrant, two
26 numbers were listed for DJOKO: (206) 430-4163 and (206) 457-0982. The 0982
27 number was also the number for DJOKO that KAMDEM provided to SPD officers
28 during a post-arrest interview. The mobile number of (206) 549-9854 was the number

1 assigned to the cell phone seized from DJOKO when he was arrested on November 10,
2 2018. Based on my training and experience, I know that individuals involved in criminal
3 activity often maintain multiple cellular phones and/or replace phones they believe will
4 implicate them in criminal acts.

5 22. Because KAMDEM and DJOKO are both frequent users of cell phone-
6 enabled text messaging, I believe that the geolocation data requested is relevant and
7 material to the ongoing criminal investigation and will likely reveal fruits, contraband,
8 instrumentalities, or evidence of violation of Title 18, United States Code, Sections of
9 249 (hate crimes), 370 (conspiracy) and 2261A (Stalking).

10 **IV. Specialized Information from Target Cell Phones**

11 23. In my training and experience, I have learned that T-Mobile and Onvoy
12 LLC are companies that provide cellular telephone access to the general public. I also
13 know that providers of cellular telephone service have technical capabilities that allow
14 them to collect and generate at least two kinds of information about the locations of the
15 cellular telephones to which they provide service: (1) E-911 Phase II data, also known as
16 GPS data or latitude-longitude data, and (2) cell-site data, also known as "tower/face
17 information" or cell tower/sector records. E-911 Phase II data provides relatively precise
18 location information about the cellular telephone itself, either via GPS tracking
19 technology built into the phone or by triangulating on the device's signal using data from
20 several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e.,
21 antenna towers covering specific geographic areas) that received a radio signal from the
22 cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the
23 telephone connected. These towers are often a half-mile or more apart, even in urban
24 areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to
25 a wireless device does not necessarily serve every call made to or from that device.
26 Accordingly, cell-site data is typically less precise than E-911 Phase II data.

27 24. Based on my training and experience, I know that providers of cell service
28 such as T-Mobile can collect E-911 Phase II data about the location of the **Target Cell**

1 **Phones**, including by initiating a signal to determine the location of the **Target Cell**
2 **Phones** on the provider's network or with such other reference points as may be
3 reasonably available.

4 25. Based on my training and experience, I know that providers such as T-
5 Mobile can collect cell-site data about the **Target Cell Phones**.

6 26. In my training and experience, I have learned that cellular phones and other
7 cellular devices communicate wirelessly across a network of cellular infrastructure,
8 including towers that route and connect individual communications. When sending or
9 receiving a communication, a cellular device broadcasts certain signals to the cellular
10 tower that is routing its communication. These signals include a cellular device's unique
11 identifiers.

12 27. I believe the collection of E-911 Phase II data and cell-site data related to
13 the **Target Cell Phones** has relevant information related to the crimes against John Doe.
14 Specifically, it will show the location of the **Target Cell Phones** on the date that John
15 Doe was assaulted leading up to and shortly after the assault, including the defacement of
16 John Doe's vehicle and harassing text messages sent and received during the time period
17 of October 20, 2018, to October 27, 2018

18 **V. Information To Be Searched And Things To Be Seized**

19 28. Pursuant to Title 18, United States Code, Section 2703(g), this application
20 and affidavit for search warrants seek authorization to permit T-Mobile Wireless, and
21 Onvoy LLC, and its agents and employees, to assist agents in the execution of this
22 warrant. Once issued, the search warrants will be presented to T-Mobile and Onvoy
23 LLC, with direction that they identify the accounts described in Attachments A-1 and A-2
24 to this affidavit, respectively, as well as other subscriber and log records associated with
25 the account, as set forth in Attachments B to this Affidavit.

26 29. The search warrants will direct T-Mobile and Onvoy LLC to create an
27 exact copy of the specified account and records, including an exact copy of the contents
28

1 of the hard disk drive or drives installed on the server associated with the **Target Cell**
2 **Phones**, or the original drives.

3 30. I, and/or other law enforcement personnel will thereafter review the copy of
4 the electronically stored data, and identify from among that content those items that come
5 within the items identified in Attachment B, for seizure.

6 31. Analyzing the data contained in the forensic image may require special
7 technical skills, equipment, and software. It could also be very time-consuming.
8 Searching by keywords, for example, can yield thousands of "hits," each of which must
9 then be reviewed in context by the examiner to determine whether the data is within the
10 scope of the warrant. Merely finding a relevant "hit" does not end the review process.
11 Keywords used originally need to be modified continuously, based on interim results.
12 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,
13 search text, and many common e-mail, database and spreadsheet applications do not store
14 data as searchable text. The data may be saved, instead, in proprietary non-text format.
15 And, as the volume of storage allotted by service providers increases, the time it takes to
16 properly analyze recovered data increases, as well. Consistent with the foregoing,
17 searching the recovered data for the information subject to seizure pursuant to this
18 warrant may require a range of data analysis techniques and may take weeks or even
19 months. All forensic analysis of the data will employ only those search protocols and
20 methodologies reasonably designed to identify and seize the items identified in
21 Attachment B to the warrant.

22 VI. REQUEST FOR DELAYING NOTICE

23 32. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of
24 Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to
25 delay notice until 60 days after the collection authorized by the warrant has been
26 completed. This delay is justified because there is reasonable cause to believe that
27 providing immediate notification of the warrant may have an adverse result, as defined in
28 18 U.S.C. § 2705. Based upon my knowledge, training, and experience, it is my belief

1 that providing immediate notice to subscriber or user(s) of the **Target Cell Phones** may
2 result in premature notification to DJOKO, the subscriber, or other as yet unknown users
3 of the existence of the authorization for telephone location tracking would alert them to
4 the ongoing investigation, and this disclosure would jeopardize the continuation and
5 efficacy of the investigation. For example, two of the Target Cell Phones, specifically
6 the phones assigned numbers (206) 430-4163 and 206-457-0982, are not in law
7 enforcement custody. Premature notice of the warrant may jeopardize collection of
8 additional evidence and/or destruction of evidence relating to those cell phones.
9 Furthermore, premature notification to DJOKO, the subscriber, or unknown users of the
10 existence of the authorization for telephone location tracking prior to completion of the
11 investigation would provide them with the opportunity to destroy evidence and flee the
12 jurisdiction. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which
13 is incorporated into the warrant, the proposed search warrant does not authorize the
14 seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent
15 that the warrant authorizes the seizure of any wire or electronic communication (as
16 defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is
17 reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. §
18 3103a(b)(2).

19 VII. REQUEST FOR SEALING

20 33. I further request this Court issue an order sealing, until further order of the
21 Court, all papers submitted in support of the requested search warrant, including the
22 application, this affidavit, the attachments, and the requested search warrant. I believe
23 sealing these documents is necessary because the information to be seized is relevant to
24 an ongoing investigation, and any disclosure of the information at this time may cause
25 DJOKO, or others associated with **Target Cell Phones**, to flee from prosecution, cause
26 destruction of or tampering with evidence, or otherwise seriously jeopardize this
27 investigation. Premature disclosure of the contents of the application, this affidavit, the
28

1 attachments, and the requested search warrant may adversely affect the integrity of the
2 investigation.


3 **VIII. CONCLUSION**

4 34. Based on the foregoing, I request that the Court issue the proposed search
5 warrants, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). I
6 further request that the Court authorize execution of the warrant at any time of day or
7 night, owing to the potential need to locate the information relating to the Target Cell
8 Phones as identified in Attachment B, outside of daytime hours. Pursuant to 18 U.S.C. §
9 2703(g), the presence of a law enforcement officer is not required for the service or
10 execution of this warrant. Accordingly, by this Affidavit and warrant I seek authority for
11 the government to search and seize all of the data, documents and records specified in
12 Attachment B (attached hereto and incorporated by reference herein) to the warrant.

13 35. I further request that the Court direct Provider to disclose to the government
14 any information described in Attachment B that is within the possession, custody, or
15 control of Provider. I also request that the Court direct Provider to furnish the
16 government all information, facilities, and technical assistance necessary to accomplish
17 the collection of the information described in Attachment B unobtrusively and with a
18 minimum of interference with Provider's services, including by initiating a signal to
19
20
21
22
23
24
25
26
27
28

1 determine the location of the **Target Cell Phones** on Providers' network or with such
2 other reference points as may be reasonably available, and at such intervals and times
3 directed by the government.

4 Dated this 6th day of November 2019.

5 
6 _____
7 Greg Leiman
8 Special Agent
9 Federal Bureau of Investigations

10 SUBSCRIBED AND SWORN to before me this 6th day of November, 2019.

11 
12 _____
13 MICHELLE L. PETERSON
14 United States Magistrate Judge
15
16
17
18
19
20
21
22
23
24
25
26
27
28